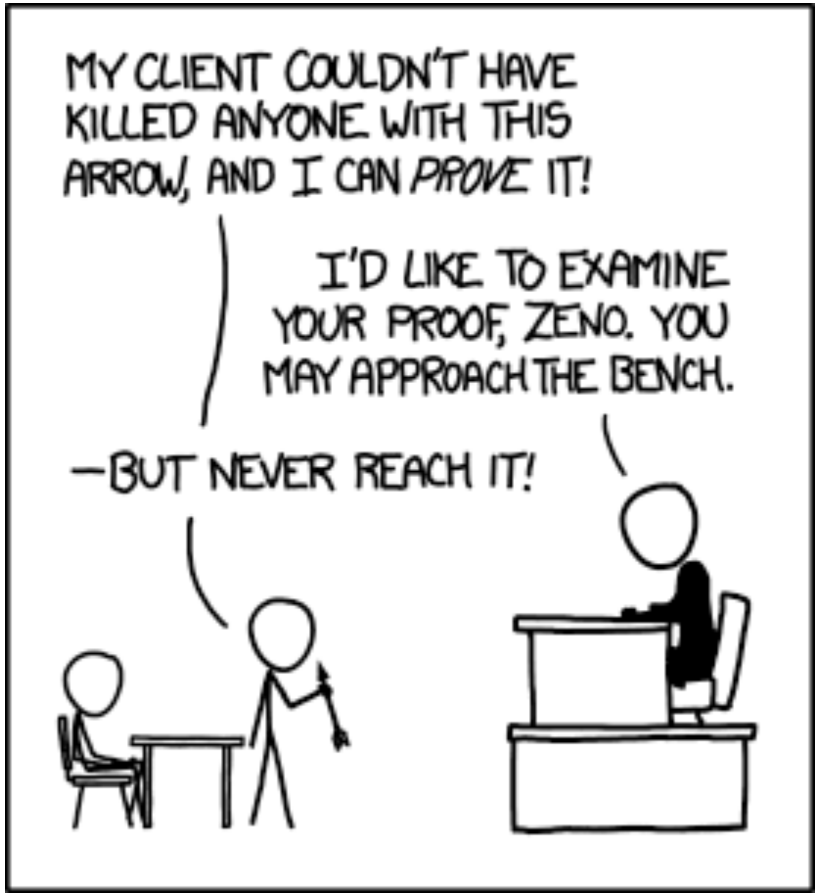

xkcd.com/1153

Reminder: pollev.com/cse311

Download activity slides from homepage

Our First Proof and Digital Logic

CSE 311 Fall 2020
Lecture 3

Law of Implication

Implications are not totally intuitive.
AND/OR/NOT make more intuitive sense to me…
can we rewrite implications using just ANDs ORs and NOTs?

a	b	$\boxed{a \to b}$
T	T	T
T	F	F
F	T	T
F	F	T

Vacuous truths

Seems like we might want $\neg(a \wedge \neg b)$

$\neg a \vee b$

Seems like a reasonable guess.
So is it true? Is $\boxed{\neg a \vee b} \boxed{\equiv} a \to b$?

Law of Implication

$$\neg a \lor b \equiv a \to b$$

$a \leftrightarrow b$

$\boldsymbol{a}$	b	$a \to b$	$\neg a$	$\neg a \lor b$	$\boxed{(\neg a \lor b) \leftrightarrow (a \to b)}$
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Warm-Up

"I go to the store, unless I order postmates."

a b

How would you translate "unless" into logic?

$a \vee (\neg a \wedge b)$

$\neg a \rightarrow b$

$\neg b \rightarrow a$

are these $\equiv$?

"If I don't go to the store, then I order postmates"

Today

Our first proof!

Contrapositives and digital logic.

Announcements

Homework 1 Problem 6 clarified (download a new version of the pdf).

Office Hours start this week.

Homework Submissions

Make sure we can read what you submit.

We can't spend 5 minutes per submission deciding if that's a p or a q.

Typesetting guarantees we can read it.

Microsoft Word's ebuation editor is now halfway decent!

LaTeX is the industry standard for typesetting (if you go to CS grad school, you'll use it for all your papers). Overleaf is the easiest way to get started.

Need to know the code for a symbol? Detexify! Word uses LaTeX codes…mostly…

Our First Proof

Last Time

We showed

DeMorgan's Laws:

$\neg(a \vee b) \equiv \neg a \wedge \neg b$ and $\neg(a \wedge b) \equiv \neg a \vee \neg b$

And the Law of Implication

$\boxed{a \rightarrow b \equiv \neg a \vee b}$

Properties of Logical Connectives

We will always give you this list!

Try truth tables

For every propositions a, b, r the following hold:

- Identity
  - $a \wedge \mathrm{T} \equiv a$
  - $a \vee \mathrm{F} \equiv a$
- Domination
  - $a \wedge \mathrm{F} \equiv \mathrm{F}$
  - $a \vee \mathrm{T} \equiv \mathrm{T}$
- Idempotent
  - $a \vee a \equiv a$
  - $a \wedge a \equiv a$
- Communtative
  - $a \wedge b \equiv b \wedge a$
  - $a \vee b \equiv b \vee a$
- Associative
  - $(a \vee b) \vee r \equiv a \vee (b \vee r)$
  - $(a \wedge b) \wedge r \equiv a \wedge (b \wedge r)$
- Distributive
  - $a \wedge (b \vee r) \equiv (a \wedge b) \vee (a \wedge r)$
  - $a \vee (b \wedge r) \equiv (a \vee\wedge b) \wedge (a \vee r)$
- Absorption
  - $a \vee (a \wedge b) \equiv a$
  - $a \wedge (a \vee b) \equiv a$
- Negation
  - $a \vee \neg a \equiv \mathrm{T}$
  - $a \wedge \neg a \equiv \mathrm{F}$

Using Our Rules

WOW that was a lot of rules.

Why do we need them? Simplification!

Let's go back to the "law of implication" example.

a	b	$a \rightarrow b$
T	T	T
T	F	F
F	T	T
F	F	T

When is the implication true? Just "or" each of the three "true" lines!

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b)$

Also seems pretty reasonable

So is $(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) \equiv (\neg a \vee b)$

i.e. are these both alternative representations of $a \rightarrow b$?

Our First Proof

We could make another truth table (you should! It's a good exercise)

But we have another technique that is nicer.

Let's try that one

Then talk about why it's another good option.

We're going to give an iron-clad guarantee that:

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) \equiv \neg a \vee b$ $\equiv a \to b$

i.e. that this is another valid "law of implication"

Our First Proof

How do we write a proof?

It’s not always plug-and-chug…we’ll be highlighting strategies throughout the quarter.

To start with:

Make sure we know what we want to show…

Our First Proof

$$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) \equiv$$

None of the rules look like this

Practice of Proof-Writing:
Big Picture…WHY do we think this might be true?

The last two "pieces" came from the vacuous proof lines…maybe the "$\neg$a" came from there? Maybe that **simplifies** down to $\neg$a

$$\equiv (\neg a \vee b)$$

Let's apply a rule

$(\neg a \land b) \lor (\neg a \land \neg b)$

The law says:

$a \land (b \lor r) \equiv (a \land b) \lor (a \land r)$

$(\neg a \land b) \lor (\neg a \land \neg b) \equiv \neg a \land (b \lor \neg b)$

Our First Proof

$(\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge \neg b) \equiv$

None of the rules look like this

Practice of Proof-Writing:
Big Picture…WHY do we think this might be true?

The last two "pieces" came from the vacuous proof lines…maybe the "$\neg\mathrm{a}$" came from there? Maybe that **simplifies** down to $\neg\mathrm{a}$

$\equiv (\neg\mathrm{a} \vee b)$

Our First Proof

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) \equiv (a \wedge b) \vee \boxed{[(\neg a \wedge b) \vee (\neg a \wedge \neg b)]}$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Associative law
Connect up the things we're working on.

$\equiv (\neg a \vee b)$

Our First Proof

"a" in our 1st dist. rule

$$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b) \equiv (a \wedge b) \vee [(\neg a \wedge b) \vee (\neg a \wedge \neg b)]$$
$$\equiv (a \wedge b) \vee [\neg a \wedge (b \vee \neg b)]$$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Distributive law
We think ¬a is important, let's isolate it.

$$\equiv (\neg a \vee b)$$

Our First Proof

$(\mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge \neg b)$

$$\equiv (\mathrm{a} \wedge b) \vee [(\neg \mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge \neg b)]$$
$$\equiv (\mathrm{a} \wedge b) \vee [\neg \mathrm{a} \wedge (b \vee \neg b)]$$
$$\equiv (\mathrm{a} \wedge b) \vee [\neg \mathrm{a} \wedge \mathrm{T}]$$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Negation
Should make things simpler.

$$\equiv (\neg \mathrm{a} \vee b)$$

Our First Proof

$(\mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge \neg b)$

$\equiv (\mathrm{a} \wedge b) \vee [(\neg \mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge \neg b)]$

$\equiv (\mathrm{a} \wedge b) \vee [\neg \mathrm{a} \wedge (b \vee \neg b)]$

$\equiv (\mathrm{a} \wedge b) \vee [\neg \mathrm{a} \wedge \mathrm{T}]$

$\equiv (\mathrm{a} \wedge b) \vee [\neg \mathrm{a}]$

Set ourselves an intermediate goal.
Let's try to simplify those last two pieces

Domination
Should make things simpler.

$\equiv (\neg \mathrm{a} \vee b)$

Our First Proof

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b)$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg a \vee b)$

If we apply the distribution rule,
We'd get a $(\neg a \vee b)$

$$\begin{aligned}
&\equiv (a \wedge b) \vee [(\neg a \wedge b) \vee (\neg a \wedge \neg b)] \\
&\equiv (a \wedge b) \vee [\neg a \wedge (b \vee \neg b)] \\
&\equiv (a \wedge b) \vee [\neg a \wedge T] \\
&\equiv (a \wedge b) \vee [\neg a] \\
&\equiv [\neg a] \vee (a \wedge b)
\end{aligned}$$

$$\equiv (\neg a \vee b)$$

Our First Proof

$$(\mathrm{a} \land b) \lor (\neg\mathrm{a} \land b) \lor (\neg\mathrm{a} \land \neg b)$$

$$\begin{aligned}
&\equiv (\mathrm{a} \land b) \lor [(\neg\mathrm{a} \land b) \lor (\neg\mathrm{a} \land \neg b)] \\
&\equiv (\mathrm{a} \land b) \lor [\neg\mathrm{a} \land (b \lor \neg b)] \\
&\equiv (\mathrm{a} \land b) \lor [\neg\mathrm{a} \land \mathrm{T}] \\
&\equiv (\mathrm{a} \land b) \lor [\neg\mathrm{a}] \\
&\equiv [\neg\mathrm{a}] \lor (\mathrm{a} \land b)
\end{aligned}$$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg\mathrm{a} \lor b)$

If we apply the distribution rule,
We'd get a $(\neg\mathrm{a} \lor b)$

$$\equiv (\neg\mathrm{a} \lor b)$$

Commutative
Make the expression look exactly like the law (more on this later)

Our First Proof

$(\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge \neg b)$

$$
\begin{aligned}
&\equiv (\mathrm{a} \wedge b) \vee [(\neg\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge \neg b)] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a} \wedge (b \vee \neg b)] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a} \wedge \mathrm{T}] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a}] \\
&\equiv [\neg\mathrm{a}] \vee (\mathrm{a} \wedge b) \\
&\equiv (\neg\mathrm{a} \vee \mathrm{a}) \wedge (\neg\mathrm{a} \vee b)
\end{aligned}
$$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg\mathrm{a} \vee b)$

If we apply the distribution rule,
We'd get a $(\neg\mathrm{a} \vee b)$

Distributive $\equiv (\neg\mathrm{a} \vee b)$

Creates the $(\neg\mathrm{a} \vee b)$ we were hoping for.

Our First Proof

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b)$

$\equiv (a \wedge b) \vee [(\neg a \wedge b) \vee (\neg a \wedge \neg b)]$

$\equiv (a \wedge b) \vee [\neg a \wedge (b \vee \neg b)]$

$\equiv (a \wedge b) \vee [\neg a \wedge T]$

$\equiv (a \wedge b) \vee [\neg a]$

$\equiv [\neg a] \vee (a \wedge b)$

$\equiv (\neg a \vee a) \wedge (\neg a \vee b)$

$\equiv (a \vee \neg a) \wedge (\neg a \vee b)$

$\equiv T \wedge (\neg a \vee b)$

$\equiv (\neg a \vee b)$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg a \vee b)$

If we apply the distribution rule,
We'd get a $(\neg a \vee b)$

Commutativ

$\equiv (\neg a \vee b) \wedge$
T

$\equiv \neg a \vee b$

Commutative
Make the expression look exactly like the law (more on this later)

Negation
Simplifies the part we want to disappear.

Simplify $\mathtt{T} \wedge (\neg a \vee b)$ to $(\neg a \vee b)$

For every propositions a, b, r the following hold:

- Identity
  - $a \wedge \mathrm{T} \equiv a$
  - $a \vee \mathrm{F} \equiv a$
- Domination
  - $a \wedge \mathrm{F} \equiv \mathrm{F}$
  - $a \vee \mathrm{T} \equiv \mathrm{T}$
- Idempotent
  - $a \vee a \equiv a$
  - $a \wedge a \equiv a$
- Communtative
  - $a \wedge b \equiv b \wedge a$
  - $a \vee b \equiv b \vee a$
- Associative
  - $(a \vee b) \vee r \equiv a \vee (b \vee r)$
  - $(a \wedge b) \wedge r \equiv a \wedge (b \wedge r)$
- Distributive
  - $a \wedge (b \vee r) \equiv (a \wedge b) \vee (a \wedge r)$
  - $a \vee (b \wedge r) \equiv (a \vee\wedge b) \wedge (a \vee r)$
- Absorption
  - $a \vee (a \wedge b) \equiv a$
  - $a \wedge (a \vee b) \equiv a$
- Negation
  - $a \vee \neg a \equiv \mathrm{T}$
  - $a \wedge \neg a \equiv \mathrm{F}$

Properties of Logical Connectives

We will always give you this list!

For every propositions a, b, r the following hold:

- Identity
  - $a \wedge \mathrm{T} \equiv a$
  - $a \vee \mathrm{F} \equiv a$
- Domination
  - $a \wedge \mathrm{F} \equiv \mathrm{F}$
  - $a \vee \mathrm{T} \equiv \mathrm{T}$
- Idempotent
  - $a \vee a \equiv a$
  - $a \wedge a \equiv a$
- Communtative
  - $a \wedge b \equiv b \wedge a$
  - $a \vee b \ \equiv b \vee a$
- Associative
  - $(a \vee b) \vee r \equiv a \vee (b \vee r)$
  - $(a \wedge b) \wedge r \equiv a \wedge (b \wedge r)$
- Distributive
  - $a \wedge (b \vee r) \equiv (a \wedge b) \vee (a \wedge r)$
  - $a \vee (b \wedge r) \equiv (a \vee\wedge b) \wedge (a \vee r)$
- Absorption
  - $a \vee (a \wedge b) \equiv a$
  - $a \wedge (a \vee b) \equiv a$
- Negation
  - $a \vee \neg a \equiv \mathrm{T}$
  - $a \wedge \neg a \ \equiv \mathrm{F}$

Our First Proof

$(\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge \neg b)$

$$
\begin{aligned}
&\equiv (\mathrm{a} \wedge b) \vee [(\neg\mathrm{a} \wedge b) \vee (\neg\mathrm{a} \wedge \neg b)] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a} \wedge (b \vee \neg b)] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a} \wedge \mathrm{T}] \\
&\equiv (\mathrm{a} \wedge b) \vee [\neg\mathrm{a}] \\
&\equiv [\neg\mathrm{a}] \vee (\mathrm{a} \wedge b) \\
&\equiv (\neg\mathrm{a} \vee \mathrm{a}) \wedge (\neg\mathrm{a} \vee b) \\
&\equiv (\mathrm{a} \vee \neg\mathrm{a}) \wedge (\neg\mathrm{a} \vee b) \\
&\equiv \mathrm{T} \wedge (\neg\mathrm{a} \vee b) \\
&\equiv (\neg\mathrm{a} \vee b) \wedge \mathrm{T} \\
&\equiv (\neg\mathrm{a} \vee b)
\end{aligned}
$$

Stay on target:
We met our intermediate goal.
Don't forget the final goal!
We want to end up at $(\neg\mathrm{a} \vee b)$

If we apply the distribution rule,
We'd get a $(\neg\mathrm{a} \vee b)$

Commutative followed by **Domination**
Look exactly like the law, then apply it.

We're done!!!

Commutativity

We had the expression $(\mathrm{a} \wedge b) \vee [\neg \mathrm{a}]$

But before we applied the distributive law, we switched the order…why?

The law says $\mathrm{a} \vee (b \wedge r) \equiv (\mathrm{a} \vee b) \wedge (\mathrm{a} \vee r)$

not $(b \wedge r) \vee \mathrm{a} \equiv (b \vee \mathrm{a}) \wedge (r \vee \mathrm{a})$

So **technically** we needed to commute first.

Eventually (in about 2 weeks) we'll skip this step. For now, we're doing two separate steps.

Remember this is the "training wheel" stage. The point is to be careful.

More on Our First Proof

We now have an ironclad guarantee that

$(\mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge b) \vee (\neg \mathrm{a} \wedge \neg b) \equiv (\neg \mathrm{a} \vee b)$

Hooray! But we could have just made a truth-table. Why a proof?

Here's one reason.

Proofs don't *just* give us an ironclad guarantee. They're also an explanation of *why* the claim is true.

The key insight to our simplification was "the last two pieces were the vacuous truth parts – the parts where p was false"

That's in there, *in the proof*.

Our First Proof

$(a \wedge b) \vee (\neg a \wedge b) \vee (\neg a \wedge \neg b)$

$\equiv (a \wedge b) \vee [(\neg a \wedge b) \vee (\neg a \wedge \neg b)]$	Associative
$\equiv (a \wedge b) \vee [\neg a \wedge (b \vee \neg b)]$	Distributive
$\equiv (a \wedge b) \vee [\neg a \wedge T]$	Negation
$\equiv (a \wedge b) \vee [\neg a]$	Domination
$\equiv [\neg a] \vee (a \wedge b)$	Commutative
$\equiv (\neg a \vee a) \wedge (\neg a \vee b)$	Distributive
$\equiv (a \vee \neg a) \wedge (\neg a \vee b)$	Commutative
$\equiv T \wedge (\neg a \vee b)$	Negation
$\equiv (\neg a \vee b) \wedge T$	Commutative
$\equiv (\neg a \vee b)$	Domination

The last two terms are "vacuous truth" – they simplify to ¬a

p no longer matters in a ∧ b if ¬a automatically makes the expression true.

More on Our First Proof

With practice (and quite a bit of squinting) you can see not just the ironclad guarantee, but also the reason why something is true.

That's not easy with a truth table.

Proofs can also communicate intuition about why a statement is true.

- We'll practice extracting intuition from proofs more this quarter.

Converse, Contrapositive

Implication:

If it's raining, then I have my umbrella. $a \to b$

Contrapositive:

$\neg b \to \neg a$ If I don't have my umbrella, then it is not raining.

Converse:

If I have my umbrella, then it is raining. $b \to a$

Inverse:

$\neg a \to \neg b$ If it is not raining, then I don't have my umbrella.

How do these relate to each other?

a	b	$a \to b$	$b \to a$	$\neg a$	$\neg b$	$\neg a \to \neg b$	$\neg b \to \neg a$
T	T						
T	F						
F	T						
F	F						

Converse, Contrapositive

Implication:

$$a \rightarrow b$$

Converse:

$$b \rightarrow a$$

Contrapositive:

$$\neg b \rightarrow \neg a$$

Inverse:

$$\neg a \rightarrow \neg b$$

An implication and its contrapositive have the same truth value!

a	b	$a \rightarrow b$	$b \rightarrow a$	$\neg a$	$\neg b$	$\neg a \rightarrow \neg b$	$\neg b \rightarrow \neg a$
T	T	T	T	F	F	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Contrapositive

Activity

We showed $a \rightarrow b \equiv \neg b \rightarrow \neg a$ with a truth table. Let's do a proof.

Try this one on your own. Remember

1. Know what you're trying to show.
2. Stay on target – take steps to get closer to your goal.

Hint: think about your tools. There are lots of rules with AND/OR/NOT, but very few with implications…

Contrapositive

$a \to b \equiv \neg a \vee b$	Law of Implication
$\equiv b \vee \neg a$	Commutativity
$\equiv \neg\neg b \vee \neg a$	Double Negation
$\equiv \neg b \to \neg a$	Law of Implication

All of our rules deal with ORs and ANDs, let's switch the implication to just use AND/NOT/OR.

And do the same with our target

It's ok to work from both ends. In fact it's a very common strategy!

Now how do we get the top to look like the bottom?

Just a few more rules and we're done!

Computing Equivalence

Given two propositions, can we write an algorithm to determine if they are equivalent?

What is the runtime of our algorithm?

Computing Equivalence

Given two propositions, can we write an algorithm to determine if they are equivalent?

Yes! Generate the truth tables for both propositions and check if they are the same for every entry.

What is the runtime of our algorithm?

Every atomic proposition has two possibilities (T, F). If there are n atomic propositions, there are 2^n rows in the truth table.